УДК 004.732.056 **DOI: 10.20998/2411-0558.2016.21.13**

С.Г. СЕМЕНОВ, д-р техн. наук, с.н.с.., зав. каф., НТУ "ХПИ",
С.Ю. ГАВРИЛЕНКО, канд. техн. наук, доц., НТУ "ХПИ",
В.В. ЧЕЛАК, студент, НТУ "ХПИ"

РАЗРАБОТКА ШАБЛОНОВ ИДЕНТИФИКАЦИИ СОСТОЯНИЯ КОМПЬЮТЕРНЫХ СИСТЕМ НА ОСНОВЕ BDS-ТЕСТИРОВАНИЯ

В статье разработаны шаблоны фиксации аномального поведения компьютерных систем на основе BDS-тестов. Разработана имитационная модель, при этом ее входными данными стали показатели загрузки центрального процессора, оперативной памяти и их соотношения. Полученные результаты исследований позволяют сделать вывод о возможности использования разработанных шаблонов фиксации аномального поведения компьютерных систем на основе BDS-тестирования в эвристических анализаторах систем обнаружения вторжений. Ил.: 2. Табл.: 2. Библиогр.: 10 назв.

Ключевые слова: компьютерные системы, шаблоны фиксации аномального поведения, BDS-тест.

Постановка проблемы. Одна из главных причин потерь компьютерной информации в наше время связана с деятельностью вредоносных программ. На протяжении года вирусы наносят убытки на десятки миллиардов долларов и еще, приблизительно столько же, составляют непрямые убытки, связанные с разработкой программного обеспечения и проведения других мероприятий защиты от вирусов.

При решении задач, связанных с диагностикой и защитой компьютерных информационных ресурсов, центральной является задача оперативного выявления аномального поведения компьютерных систем (КС) в условиях вирусных атак.

Известно, что в настоящее время для решения сложной задачи антивирусной защиты данных используется множество специализированных антивирусных программ, в основу которых, чаще всего, входят сигнатурные и эвристические анализаторы.

Эвристические анализаторы, как правило, включают в себя интеллектуальные подсистемы, базирующиеся на теории искусственного интеллекта, например, на основе методов нечеткой логики, кластерного анализа, согласованных эвристик или теории нейронных сетей. В то же время все они основаны на предположении, что для КС существует свой шаблон нормального поведения и любые значительные отклонения от него могут быть обусловлены воздействием злоумышленников. Именно поэтому очень важной задачей является выбор или формирование такого шаблона, который бы воспроизводил функциональный портрет КС и

фиксировал аномальное ее поведение с заданной точностью.

Анализ литературы показал, что для обнаружения аномалий в управлении производством, бизнес-процессами широко используют метод контрольных карт. Для построения шаблона нормальной работы системы применяются контрольные карты Шухарта [1], EWMA [2] и CUSUM [3], которые используют в качестве входных данных набор показателей, характеризующий работу системы. Кроме этого, для уточнения полученных результатов дополнительно могут использоваться методы статистической обработки данных (например, BDS-тестирование [4].

Однако, как показали исследования, приведенные средства формирования шаблонов не лишены ряда недостатков. Так, например, контрольные карты EWMA нечувствительны к коротким проявлениям аномалий. В то же время карты CUSUM обнаруживают небольшие, но постоянные изменения с большей вероятностью, но обладают низкой точностью (высокой вероятностью ложных срабатываний) в случае динамических изменения показателей КС. Устранить это противоречие можно разработкой адаптивных шаблонов фиксации аномального поведения КС [5 – 9].

Таким образом, проведенный анализ существующих подходов антивирусной защиты данных показал необходимость адекватного выбора показателя аномального поведения компьютерных систем в условиях внешних воздействий и разработки критерия оценки, соответствующего выбранному показателю.

Цели статьи. Разработка новых шаблонов фиксации аномального поведения компьютерных систем.

Результаты разработки и исследований. Одним из перспективных направлений параметрического анализа является *BDS*-тестирование. *BDS*-тесты, предложенные в результате анализа финансовых рынков экономистами Броком, Дечертом и Шейнкманом (B. Brock, W. Dechert и J. Scheinkman) в 1987 году [4], и названные первыми буквами их фамилий, представляют собой эффективные методы выявления зависимостей во временных рядах в рамках их нелинейного анализа. Их цель состоит в том, чтобы различить данные I.I.D. (independent and identically distributed random variables) и любой вид зависимости – проверить нулевую гипотезу H_0 о независимости и тождественном распределении значений временного ряда $\vec{\xi} = (\xi_1, \xi_2, ..., \xi_N)$, используя для этого критерий значимости. Согласно этому критерию для принятия гипотезы H_0 необходимо выбрать критическую область G_α, удовлетворяющую условию $P(g \in G) = \alpha$, где

$g(\xi_1, \xi_2, ..., \xi_N)$ – статистика наблюдения, а α – устанавливаемый уровень значимости.

Из [2 – 5] известно, что BDS-тест основан на статистической величине $w(\vec{\xi})$ (BDS-статистике):

$$w_{m,N}(\varepsilon) = \sqrt{N-m+1}\,\frac{C_{m,N}(\varepsilon) - C_{1,N-m}(\varepsilon)^m}{\sigma_{m,N}(\varepsilon)}, \qquad (1)$$

где $C_{m,N}(\varepsilon) - C_{1,N-m}(\varepsilon)^m$ – числитель *BDS*-статистики, определяется корреляционными интегралами $C_{m,N}(\varepsilon)$, $C_{1,N-m}(\varepsilon)$ для выборки размера m; N – число элементов временного ряда; ε – радиус гиперсферы; $\sigma_{m,N}(\varepsilon)$ – среднеквадратичное отклонение разницы $C_{m,N}(\varepsilon) - C_{1,N-m}(\varepsilon)^m$.

Корреляционный интеграл определяет частоту попадания произвольной пары точек фазового пространства в гиперсферы радиуса ε:

$$C_{m,N}(\varepsilon) = \frac{2}{(N-m+1)(N-m)} \sum_{s=1}^{N-m} \left[\sum_{t=s+1}^{N-m+1} I\left(\left\| x_s^m - x_t^m \right\|\right) \right], \qquad (2)$$

где $I(x)$ – функция Хевисайда:

$$I(x) = \begin{cases} 1, & \text{если } |x| < \varepsilon, \\ 0, & \text{если } |x| \geq \varepsilon. \end{cases} \qquad (3)$$

На параметры наложено ограничение, которое обосновано в ряде работ [3 – 6]:

$$\begin{gathered} \frac{N}{m} > 200, \\ \varepsilon \in [0.5\sigma;\, \sigma], \\ I < m < 6. \end{gathered} \qquad (4)$$

BDS-тест оценивает степень хаотичности процесса. Критерием хаотичности является значение BDS-теста $\left|w_{m,N}(\varepsilon)\right| \leq 1{,}96$.

Основные положения математической формализации технологии BDS-тестирования в приложении к средствам защиты информации в компьютерных системах представлены в работах [6, 7, 10]. В то же время проведенные исследования показали, что данный критерий не отражает в полной мере результаты влияния вирусных атак на указанные выше статистические показатели.

Для выявления возможности и особенностей идентификации состояния компьютерной системы в условиях вирусных атак была разработана имитационная модель, при этом ее входными данными стали показатели загрузки центрального процессора (CPU), оперативной памяти (RAM) и их соотношения (CPU/RAM).

Модель предусматривает вариацию N – количества значений временного ряда. Значение загрузки центрального процессора сканируется ежесекундно и сохраняется в файле.

Полученные входные значения делятся на выборки по 500 значений и подаются на вход модуля анализа, который обрабатывает и анализирует данные с помощью BDS-статистики. Результатом работы программной модели является N/500 значений BDS-теста.

Результаты значений BDS-теста для различных режимов работы системы приведены в табл. 1, 2.

Таблица 1

Значение BDS-теста для CPU для различных режимов работы системы (Режим 1 – 3 – нормальный, режим 4 – 6 – аномальный)

№	Режим 1	Режим 2	Режим 3	Режим 4	Режим 5	Режим 6
1	65,21	43,52	39,96	118,36	111,01	123,48
2	54,99	37,01	61,29	125,29	111,91	124,40
3	69,00	33,48	58,69	121,47	115,77	128,57
4	45,79	32,54	63,28	128,35	106,62	126,56
5	47,77	35,61	67,71	127,48	107,01	120,21
6	57,56	35,90	31,22	132,91	116,64	123,20
7	53,09	31,57	39,45	118,33	116,39	125,92
8	58,90	33,52	30,59	121,68	106,37	118,73
9	55,37	32,69	59,65	126,96	115,65	131,17
10	47,00	29,10	37,32	126,53	122,42	126,90
11	54,30	36,03	74,86	129,36	109,71	125,36
12	61,08	33,02	78,90	121,95	115,07	124,70
13	64,67	33,74	50,71	123,23	120,42	124,27
14	77,21	33,53	47,54	124,03	124,04	127,29
15	63,21	33,98	60,51	128,04	110,60	128,06
16	74,44	33,62	63,08	125,51	106,29	120,96
17	69,00	33,62	40,45	130,00	109,14	127,33
18	78,65	34,05	52,90	120,23	135,82	122,89
19	71,35	35,28	64,42	129,21	107,72	125,22
20	83,52	38,56	50,96	126,01	112,70	126,42
Максимум	83,52	43,52	78,90	132,91	135,82	131,17
Минимум	45,79	29,10	30,59	118,33	106,29	118,73
Джиттер	45,17	33,14	61,22	10,97	21,74	9,49

Таблица 2

Значение BDS-теста для RAM для различных режимов работы системы (Режим 1 – 3 – нормальный, режим 4 – 6 – аномальный

№	Режим 1	Режим 2	Режим 3	Режим 4	Режим 5	Режим 6
1	1759,37	58,84	24,59	124,84	122,90	154,51
2	39,64	NaN	NaN	115,27	123,62	148,61
3	25,10	162,80	NaN	131,08	127,82	127,92
4	24,85	35,33	23,11	125,95	119,98	132,04
5	31,14	50,62	NaN	130,82	132,75	140,54
6	23,78	29,17	218,81	122,32	131,80	139,37
7	25,49	69,34	24,02	133,17	122,93	138,76
8	48,90	22,63	72,14	132,47	129,44	129,27
9	37,77	25,60	33,71	128,40	127,81	157,65
10	68,83	25,22	40,69	122,85	132,47	137,09
11	38,91	23,83	NaN	126,75	125,95	137,26
12	174692,2	25,10	NaN	115,78	130,27	124,14
13	22,54	NaN	NaN	131,62	120,49	146,72
14	NaN	28,81	NaN	129,42	117,26	133,25
15	NaN	739,18	99,26	119,00	134,34	154,16
16	NaN	NaN	NaN	133,98	126,01	162,38
17	265,53	694,42	NaN	141,87	137,98	134,82
18	46,15	61,28	NaN	117,88	121,37	139,48
19	3578,07	NaN	NaN	152,63	119,82	130,03
20	NaN	NaN	NaN	140,44	131,09	157,72
Максимум	NaN	739,18	218,81	152,63	137,98	162,38
Минимум	22,54	22,63	23,11	115,27	117,26	124,14
Джиттер	99,99	96,94	89,44	24,48	15,01	23,55

Примечание: NaN – значение стремится к бесконечности.

Проанализированы 10000 посекундных значений числового ряда, размер выборки $N = 500$, $m = 2$ ($N / m > 200$) при нормальном режиме работы и в случае заражения системы компьютерным вирусом.

График значений BDS-теста для CPU при нормальной и аномальной работе приведен на рис. 1, 2.

Если проанализировать разброс значений BDS-теста CPU при нормальном режиме работы системы (рис. 1 или табл. 1), то видно, что джиттер (процент отношения разницы между максимальным и минимальным значением к максимальному значению) для режимов 1 – 3 составляет 45,17%; 33,14%; 61,22% соответственно.

Анализ разброса значений BDS-теста CPU при аномальной работе системы (рис. 2 или табл. 1), показывает уменьшение джиттера. Джиттер для аномальной работы системы для режимов 4 – 6 составляет 10,97%; 21,74%; 9,49% соответственно.

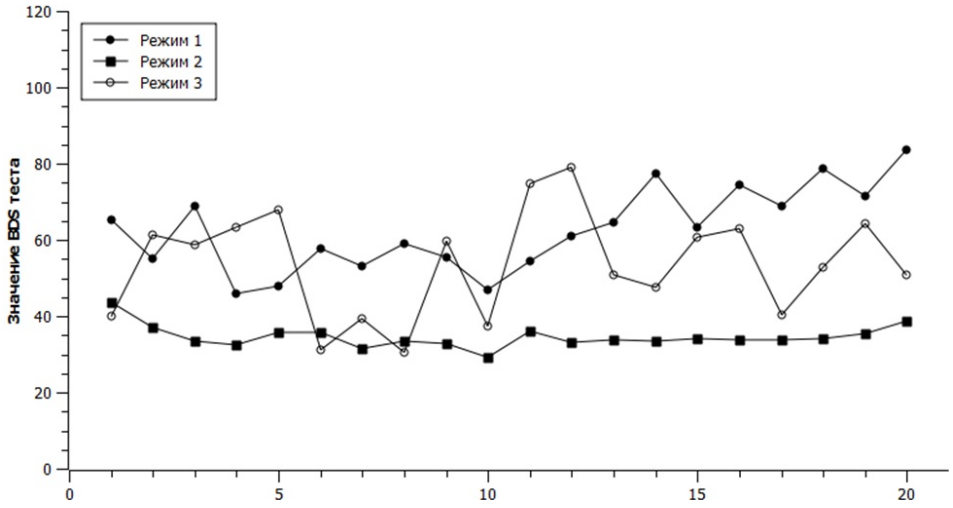

Рис. 1. График значений BDS-теста для CPU при нормальной работе системы

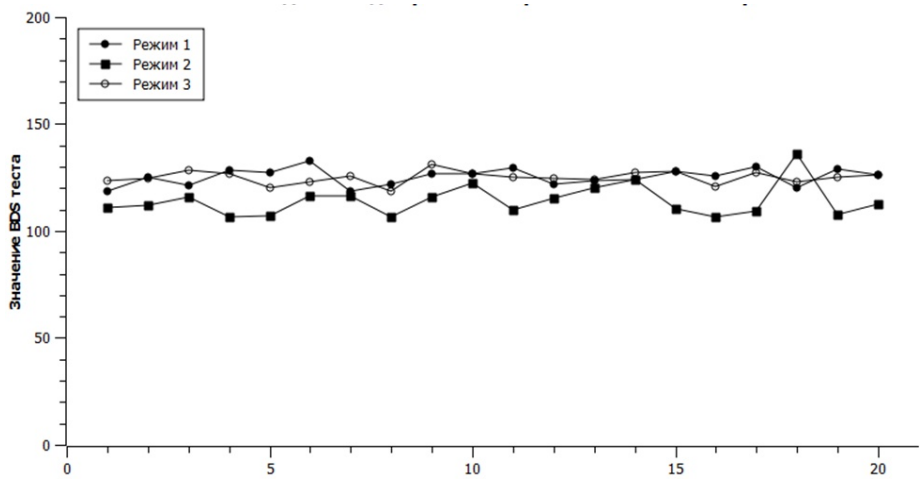

Рис. 2. График значений BDS-теста для CPU при аномальной работе системы

Вместе с тем, предыдущие исследования [10] показали, что значение BDS-статистики CPU при заражении системы вирусом fork-бомбой (программа, бесконечно создающая свои копии за счет системного вызова функции fork() и вызывающая полную загрузку процессора) стремится к 100%.

Если проанализировать разброс значений BDS-теста RAM при нормальном режиме работы системы (табл. 2), то видно что разброс параметров резко возрастает и стремиться к 100%. При аномальном

режиме работы системы (значение джиттера резко падает и находится в пределах [0% – 25%].

Аналогичные результаты значений BDS-теста получены для соотношения CPU/RAM. Значения BDS-теста для нормальной и аномальной работы системы и находятся в пределах [25% – 75%] и [0% – 25%] соответственно.

Выводы. В работе разработаны шаблоны фиксации аномального поведения компьютерных систем на основе BDS-тестирования. Для идентификации состояния компьютерной системы в условиях вирусных атак была разработана имитационная модель, при этом ее входными данными стали показатели загрузки центрального процессора, оперативной памяти и их соотношения.

Экспериментальные исследования показали, что критерием оценки нормального состояния компьютерной системы является значений BDS-теста для входных данных в интервале [25% – 75%].

Воздействие вирусов на компьютерную систему приводит к резкому снижению джиттера значений BDS-теста. Критерием аномальности является значений BDS-теста для входных данных в интервале [0% – 25%].

Вместе с тем, значение BDS-теста (для CPU и RAM) может резко возрастать в случае заражения системы вирусом или в случае использования большего количества приложений. И в первом, и во втором случае, это может быть аномальным и потребовать принятия дополнительных мер. Если причиной перегрузки CPU и RAM будет являться не вирус, то использование других методов защиты не обнаружит воздействия на компьютерную систему злоумышленного программного обеспечения.

Полученные результаты исследований позволяют сделать вывод о возможности использования разработанных шаблонов фиксации аномального поведения компьютерных систем на основе BDS-тестирования в эвристических анализаторах систем обнаружения вторжений в совокупности или каждый по отдельности.

Список литературы: **1.** Контрольні карти Шухарта. ДСТУ ISO 8258–2001 [Электронной ресурс]. – Режим доступу: http://gost-snip.su/document/dstu_iso_82582001_statistichnii_kontrol_kontrolni_karti_shuh. **2**. Общие сведения о картах кумулятивных сумм. [Электронный ресурс]. – Режим доступу: http://www.uran.donetsk.ua/~masters/2011/fimm/merkulov/library/translate.htm. **3.** Карты контроля качества. [Электронной ресурс]. – Режим доступу: http://www.statsoft.ru/home/textbook/modules/stquacon.html. **4.** *Brock W.A.* Test for independence based on the correlation dimension / *W. Brock. W. Dechert and J. Scheinkman.* – Working Paper, University of Wisconsin, 1987. **5.** *Касперский К.* Записки исследователя компьютерных вирусов / *К. Касперский*. – СПб.: Питер, 2006. – 316 с. **6.** *Шелухин О.И*. Обнаружение вторжений в компьютерные сети / *О.И. Шелухин, Д.Ж Сакалема, А.С. Филинова.* – М.:

Горячая линия – Телеком, 2013. – 220 с. **7.** *Семенов С.Г.* Защита данных в компьютеризированных управляющих системах (монография) / *С.Г. Семенов, В.В. Давыдов, С.Ю. Гавриленко.* – "LAP LAMBERT ACADEMIC PUBLISHING" Германия, 2014. – 236 с. **8.** *Порошин С.М.* Разработка и исследования математической модели компьютеризированной информационно-измерительной управляющей системы критического применения с учетом фактора внешних воздействий / *С.М. Порошин, С.Г. Семенов* // Системи обробки інформації. – Харьков: ХУ ПС. – 2013. – Вип. 2 (110). – С. 208-210. **9.** *Лукацкий А.В.* Обнаружение атак / *А.В. Лукацкий.* – Спб: BXB-Петербург, 2001. – 624 с. **10.** *Семенов С.Г.* Методы контроля и идентификации состояния компьютерных систем на основе BDS-тестирования / *С.Г. Семенов, С.Ю. Гавриленко* // Proceedings of the symposium "Metrology and metrology assurance"– Sozopol, Bulgaria, 2015. – С. 400-405.

References:

1. Shewhart control charts. DSTU ISO 8258-2001, available at: http://gost-snip.su/document/dstu_iso_82582001_statistichnii_kontrol_kontrolni_karti_shuh.
2. General information about the maps of cumulative sums, available at: http://www.uran.donetsk.ua/~masters/2011/fimm/ merkulov/library/translate.htm.
3. *Quality Control Charts*, available at: http://www.statsoft.ru/home/textbook/ modules/stquacon. html.
4. Brock W. and Dechert W. and Scheinkman. *A.,* (1987), *Test for independence based on the correlation dimension.* Working Paper, University of Wisconsin, 289 p.
5. Kaspersky K., (2006), *Notes of a computer virus researcher*, Peter, St. Petersburg, 316 p.
6. Shelukhin O.I. and Sakalema D.J. and Filinova A.S. (2013), *Intrusion Detection in Computer Networks*, Hotline-Telecom, Moscow, 220 p.
7. Semenov. S.G. and Davydov V.V. and S.Y. Gavrilenko (2014)*, Data protection in computerized control systems*, Ed. "LAP LAMBERT ACADEMIC PUBLISHING", Germany, 236 p.
8. Poroshin S.M. and Semenov S.G. (2013), "Development and research of mathematical models of the computerized information measurement control system, is taking into account factors external influences", *Information processing systems*, *HU PS*, Kharkov, Vol. 2 (110), pp. 208-210.
9. Lukatskii A.V (2001), *Intrusion Detection*, HCS-Petersburg, St. Petersburg, 624 p.
10. Semenov S.G. and Gavrilenko S.Y. (2015), "Methods of control and identification of state computer systems based on the BDS-test", Proceedings of the symposium "Metrology and metrology assurance", Sozopol, Bulgaria, pp. 400-405.

Надійшла (*received*) *12.04.2016*

Статью представил д-р техн. наук, проф. НТУ "ХПИ" Леонов С.Ю.

Semenov Sergei, Dr. Sci. Tech.
National Technical University "Kharkiv Polytechnic Institute"
Str. Kirpicheva, 21, Kharkov, Ukraine, 61002
Tel.: (057) 707-01-65, e-mail: s_semenov@ukr.net
ORCID ID: 0000-0003-4472-9234

Gavrilenko Svitlana, Cand. Sci. Tech.
National Technical University "Kharkiv Polytechnic Institute"
Str. Kirpicheva, 21, Kharkov, Ukraine, 61002

Tel.: (057) 707-01-65, e-mail: gavrilenko08@gmail.com
ORCID ID: 0000-0006-4561-8368

ChelackVictor, Student
National Technical University "Kharkiv Polytechnic Institute"
Str. Kirpicheva, 21, Kharkov, Ukraine, 61002
Tel.: (057) 707-01-65, e-mail: Victor.Chelak@gmail.com
ORCID ID: 0000-0006-4561-8368

УДК 004.732.056

Розробка шаблонів ідентифікації стану комп'ютерних систем на основі BDS-тестування / Семенов С.Г., Гавриленко С.Ю., Челак В.В. // Вісник НТУ "ХПІ". Серія: Інформатика та моделювання. – Харків: НТУ "ХПІ". – 2016. – № 21 (1193). – С. 118 – 127.

У статті розроблені шаблони фіксації аномальної поведінки комп'ютерних систем на основі BDS-тестів. Розроблено імітаційну модель, при цьому її вхідними даними стали показники завантаження центрального процесора, оперативної пам'яті і їх співвідношення. Отримані результати досліджень дозволяють зробити висновок про можливість використання розроблених шаблонів фіксації аномального поведінки комп'ютерних систем на основі BDS-тестування в евристичних аналізаторах систем виявлення вторгнень. Іл .: 2. Табл.: 2. Бібліогр .: 10 назв.

Ключові слова: комп'ютерні системи, шаблони фіксації аномальної поведінки, BDS-тест.

УДК 004.732.056

Разработка шаблонов идентификации состояния компьютерных систем на основе BDS-тестирования / Семенов С.Г., Гавриленко С.Ю., Челак В.В. // Весник НТУ "ХПИ". Серия: Информатика и моделирование. – Харьков: НТУ "ХПИ". – 2016. – № 21 (1193). – С. 118 – 127.

В статье разработаны шаблоны фиксации аномального поведения компьютерных систем на основе BDS-тестов. Разработана имитационная модель, при этом ее входными данными стали показатели загрузки центрального процессора, оперативной памяти и их соотношения. Полученные результаты исследований позволяют сделать вывод о возможности использования разработанных шаблонов фиксации аномального поведения компьютерных систем на основе BDS-тестирования в эвристических анализаторах систем обнаружения вторжений. Ил.: 2. Табл.: 2. Библиогр.: 10 назв.

Ключевые слова: компьютерные системы, шаблоны фиксации аномального поведения, BDS-тест.

UDC **004.732.056**

Design templates for identification state of computer systems are based on BDS-test / Semenov S.G, S. Yu. Gavrilenko, V.V Chelak // Herald of the National Technical University "KhPI". Subject issue: Information Science and Modelling. – Kharkov: NTU "KhPI". – 2016. – № 21 (1193). – P. 118 – 127.

In this paper are designed templates for fixing the anomalous behavior of the computer system based on BDS-test. The imitation model was developed and CPU load, memory and their ratio are input data for this model. The results suggest the possibility of using designed templates for fixing the anomalous behavior of computer systems based on the BDS-testing in the detection systems intrusion of the heuristic analyzers. Figs.: 2. Tabl.: 2. Refs.: 10 titles.

Keywords: computer systems, templates for fixing anomalous behavior, BDS-test.